Κατευθυντήριες γραμμές



Κατευθυντήριες γραμμές 04/2020 για τη χρήση δεδομένων θέσης και εργαλείων ιχνηλάτησης επαφών στο πλαίσιο της έξαρσης της νόσου COVID-19

Εγκρίθηκαν στις 21 Απριλίου 2020

Εγκρίθηκαν

Ιστορικό εκδόσεων

Έκδοση 1.1	5 Μαΐου 2020	Διορθώσεις ήσσονος σημασίας
Έκδοση 1.0	21 Απριλίου 2020	Έγκριση κατευθυντηρίων γραμμών

Πίνακας περιεχομένων

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Έχοντας υπόψη το άρθρο 70 παράγραφος 1 στοιχείο ε) του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (στο εξής: ΓΚΠΔ),

Έχοντας υπόψη τη συμφωνία για τον ΕΟΧ, και ιδίως το παράρτημα XI και το πρωτόκολλο 37 αυτής, όπως τροποποιήθηκαν με την απόφαση αριθ. 154/2018 της Μεικτής Επιτροπής του ΕΟΧ της 6ης Ιουλίου 2018[1],

Έχοντας υπόψη τα άρθρα 12 και 22 του κανονισμού του,

ΕΞΕΔΩΣΕ ΤΙΣ ΑΚΟΛΟΥΘΕΣ ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ:

1 ΕΙΣΑΓΩΓΗ ΚΑΙ ΠΛΑΙΣΙΟ

1 Οι κυβερνήσεις και οι ιδιωτικοί φορείς στρέφονται προς τη χρήση λύσεων που βασίζονται στα δεδομένα ως μέρος της απάντησης στην πανδημία COVID-19, γεγονός που εγείρει πολλές ανησυχίες για την προστασία της ιδιωτικής ζωής.

2 Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ) υπογραμμίζει ότι το νομικό πλαίσιο για την προστασία των δεδομένων σχεδιάστηκε για να έχει ευελιξία, οπότε είναι σε θέση να συμβάλλει αποτελεσματικά στον περιορισμό της πανδημίας και να εγγυηθεί την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών του ανθρώπου.

3 Το ΕΣΠΔ πιστεύει ακράδαντα ότι, όταν η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι αναγκαία για τη διαχείριση της πανδημίας COVID-19, η προστασία των δεδομένων είναι απολύτως απαραίτητη για την οικοδόμηση εμπιστοσύνης, τη δημιουργία των προϋποθέσεων για την κοινωνική αποδοχή οποιασδήποτε λύσης και, συνεπώς, για την εγγύηση της αποτελεσματικότητας των εν λόγω μέτρων. Δεδομένου ότι ο ιός δεν γνωρίζει σύνορα, φαίνεται προτιμητέο να αναπτυχθεί μια κοινή ευρωπαϊκή προσέγγιση σε απάντηση της σημερινής κρίσης ή τουλάχιστον να διαμορφωθεί ένα διαλειτουργικό πλαίσιο.

4 Το ΕΣΠΔ γενικά θεωρεί ότι τα δεδομένα και η τεχνολογία που χρησιμοποιούνται για να βοηθήσουν στην καταπολέμηση της νόσου COVID-19 θα πρέπει να χρησιμοποιούνται για να προσφέρουν δυνατότητες, και όχι για τον έλεγχο, τον στιγματισμό ή την καταπίεση των ατόμων. Επιπλέον, παρότι τα δεδομένα και η τεχνολογία μπορούν να αποτελέσουν σημαντικά εργαλεία, έχουν εγγενείς περιορισμούς και το μόνο που μπορούν να προσφέρουν είναι το να ενισχύσουν την αποτελεσματικότητα άλλων μέτρων δημόσιας υγείας. Οι γενικές αρχές της αποτελεσματικότητας, της αναγκαιότητας και της αναλογικότητας πρέπει να αποτελούν οδηγό για κάθε μέτρο που θεσπίζουν τα κράτη μέλη ή τα θεσμικά όργανα της ΕΕ και το οποίο συνεπάγεται την επεξεργασία δεδομένων προσωπικού χαρακτήρα για την καταπολέμηση της νόσου COVID-19.

---

1 Οι αναφορές στα «κράτη μέλη» στον παρόν έγγραφο θα πρέπει να νοούνται ως αναφορές στα «κράτη μέλη του ΕΟΧ».

5 Αυτές οι κατευθυντήριες γραμμές αποσαφηνίζουν τους όρους και τις αρχές για την αναλογική χρήση των δεδομένων θέσης και των εργαλείων ιχνηλάτησης επαφών, για δύο ειδικούς σκοπούς:

- χρήση των δεδομένων θέσης για την υποστήριξη της αντιμετώπισης της πανδημίας μέσω μοντελοποίησης της διασποράς του ιού, κατά τρόπο ώστε να αξιολογηθεί η συνολική αποτελεσματικότητα των μέτρων εγκλεισμού·
- ιχνηλάτηση επαφών, με σκοπό να ειδοποιούνται τα άτομα τα οποία είχαν προσεγγίσει κάποιον που αργότερα θα διαγνωστεί επιβεβαιωμένα ως φορέας του ιού, ώστε να διακόπτεται η αλυσίδα μετάδοσης το συντομότερο δυνατό.

6 Το αν θα συμβάλουν οι εφαρμογές ιχνηλάτησης επαφών στη διαχείριση της πανδημίας εξαρτάται από πολλούς παράγοντες (π.χ. ποσοστό ατόμων που χρειάζεται να τις εγκαταστήσουν, ορισμός της «επαφής» από την άποψη της εγγύτητας και της διάρκειας, κ.λπ.). Επιπλέον, τέτοιου είδους εφαρμογές πρέπει να ενταχθούν στο πλαίσιο μιας συνολικής στρατηγικής δημόσιας υγείας για την καταπολέμηση της πανδημίας, μεταξύ άλλων με εξετάσεις και με μη ψηφιακή ιχνηλάτηση επαφών ώστε να αρθούν τυχόν αμφιβολίες. Η έναρξη διάθεσης αυτών των εφαρμογών θα πρέπει να συνοδεύεται από υποστηρικτικά μέτρα για να εξασφαλιστεί ότι οι πληροφορίες που παρέχονται στους χρήστες έχουν συγκεκριμένο πλαίσιο και ότι οι ειδοποιήσεις είναι χρήσιμες για το σύστημα δημόσιας υγείας. Διαφορετικά, οι εφαρμογές αυτές ενδέχεται να μην έχουν τα επιθυμητά αποτελέσματα.

7 Το ΕΣΠΔ τονίζει ότι ο ΓΚΠΔ και η οδηγία 2002/58/ΕΚ (στο εξής: οδηγία) περιέχουν ειδικούς κανόνες που επιτρέπουν τη χρήση ανώνυμων ή προσωπικών δεδομένων για τη στήριξη των δημόσιων αρχών και άλλων συντελεστών, σε εθνικό επίπεδο και σε επίπεδο ΕΕ, με στόχο τον έλεγχο και την ανάσχεση της διάδοσης του ιού SARS-CoV-2[2].

8 Από την άποψη αυτή, το ΕΣΠΔ έχει ήδη λάβει θέση σχετικά με το γεγονός ότι η χρήση των εφαρμογών ιχνηλάτησης επαφών θα πρέπει να είναι οικειοθελής και να μη βασίζεται στην ιχνηλάτηση των μετακινήσεων των ατόμων αλλά μάλλον σε πληροφορίες εγγύτητας μεταξύ χρηστών[3].

---

[2] Βλ. προηγούμενη δήλωση του ΕΣΠΔ για την επιδημική έξαρση της νόσου COVID-19.
[3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

2 ΧΡΗΣΗ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΘΕΣΗΣ

2.1 Πηγές των δεδομένων θέσης

9 Δύο κύριες πηγές δεδομένων θέσης διατίθενται για τη μοντελοποίηση της διασποράς του ιού και της συνολικής αποτελεσματικότητας των μέτρων εγκλεισμού:

- τα δεδομένα θέσης συλλέγονται από τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών (όπως φορείς εκμετάλλευσης κινητών τηλεπικοινωνιών) κατά την παροχή της υπηρεσίας τους· και
- τα δεδομένα θέσης που συλλέγονται από εφαρμογές των παρόχων υπηρεσιών της κοινωνίας των πληροφοριών, όταν η λειτουργία αυτών των εφαρμογών απαιτεί τη χρήση τέτοιων δεδομένων (π.χ. πλοήγηση, υπηρεσίες μεταφορών κ.λπ.).

10 Το ΕΣΠΔ υπενθυμίζει ότι τα δεδομένα θέσης[4] που συλλέγονται από παρόχους ηλεκτρονικών επικοινωνιών μπορούν να υποβληθούν σε επεξεργασία μόνο στο πλαίσιο των άρθρων 6 και 9 της οδηγίας. Αυτό σημαίνει ότι τα δεδομένα αυτά μπορούν να διαβιβάζονται σε αρχές ή άλλα τρίτα μέρη, μόνον αν έχουν ανωνυμοποιηθεί από τον πάροχο ή, αν πρόκειται για δεδομένα που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού ενός χρήστη, τα οποία δεν είναι δεδομένα μετακίνησης, με την προηγούμενη συγκατάθεση των χρηστών[5].

11 Όσον αφορά τις πληροφορίες, μεταξύ αυτών και τα δεδομένα θέσης, που συλλέγονται απευθείας από τον τερματικό εξοπλισμό, εφαρμόζεται το άρθρο 5 παράγραφος 3 της οδηγίας. Κατά συνέπεια, η αποθήκευση πληροφοριών στη συσκευή του χρήστη ή η πρόσβαση σε ήδη αποθηκευμένες πληροφορίες επιτρέπεται μόνον εάν i) ο συγκεκριμένος χρήστης έχει δώσει τη συγκατάθεσή του[6] ή ii) η αποθήκευση και/ή η πρόσβαση είναι απολύτως αναγκαία για την παροχή της υπηρεσίας της κοινωνίας των πληροφοριών την οποία έχει ζητήσει ρητά ο χρήστης.

12 Ωστόσο, σύμφωνα με το άρθρο 15, είναι δυνατές παρεκκλίσεις ως προς τα δικαιώματα και τις υποχρεώσεις που προβλέπονται στην οδηγία, όταν οι παρεκκλίσεις αυτές αποτελούν αναγκαίο, κατάλληλο και ανάλογο μέτρο σε μια δημοκρατική κοινωνία για ορισμένους στόχους[7].

13 Όσον αφορά την επαναχρησιμοποίηση των δεδομένων θέσης που συλλέγονται από πάροχο υπηρεσιών της κοινωνίας των πληροφοριών για σκοπούς μοντελοποίησης (π.χ. μέσω του λειτουργικού συστήματος ή κάποιων ήδη εγκατεστημένων εφαρμογών), πρέπει να πληρούνται επιπλέον προϋποθέσεις. Μάλιστα, όταν έχουν συλλεγεί δεδομένα σύμφωνα με το άρθρο 5 παράγραφος 3 της οδηγίας, αυτά μπορούν να υποβληθούν σε περαιτέρω επεξεργασία μόνο με την πρόσθετη συγκατάθεση του προσώπου στο οποίο αναφέρονται ή βάσει νόμου της Ένωσης ή κράτους μέλους, ο οποίος συνιστά αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση των στόχων που αναφέρονται στο άρθρο 23 παράγραφος 1 του ΓΚΠΔ[8].

2.2 Εστίαση στη χρήση ανωνυμοποιημένων δεδομένων θέσης

14 Το ΕΣΠΔ τονίζει ότι, όταν πρόκειται για τη χρήση δεδομένων θέσης, θα πρέπει πάντα να προτιμάται η επεξεργασία ανωνυμοποιημένων δεδομένων και όχι δεδομένων προσωπικού χαρακτήρα.

---

[4] Βλ. άρθρο 2 στοιχείο γ) της οδηγίας.
[5] Βλ. άρθρα 6 και 9 της οδηγίας.
[6] Η έννοια της συγκατάθεσης στην οδηγία παραμένει η ίδια με την έννοια της συγκατάθεσης στον ΓΚΠΔ και πρέπει να πληροί όλες τις απαιτήσεις της συγκατάθεσης όπως προβλέπεται στο άρθρο 4 παράγραφος 11 και στο άρθρο 7 του ΓΚΠΔ.
[7] Για την ερμηνεία του άρθρου 15 της οδηγίας, βλ. επίσης απόφαση του ΔΕΕ, της 29ης Ιανουαρίου 2008 στην υπόθεση C-275/06, Productores de Música de España (Promusicae) κατά Telefónica de España SAU.
[8] Βλ. τμήμα 1.5.3 των κατευθυντήριων γραμμών αριθ. 1/2020 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των συνδεδεμένων οχημάτων.

15 Η ανωνυμοποίηση αναφέρεται στη χρήση ενός συνόλου τεχνικών με σκοπό να καταστεί αδύνατη η σύνδεση των δεδομένων με φυσικό πρόσωπο που έχει ταυτοποιηθεί ή μπορεί να ταυτοποιηθεί με «εύλογες» προσπάθειες. Αυτός ο έλεγχος «εύλογου χαρακτήρα» πρέπει να λαμβάνει υπόψη τόσο αντικειμενικές πτυχές (χρόνος, τεχνικά μέσα κ.λπ.) όσο και συγκυριακά στοιχεία που μπορεί να διαφέρουν ανάλογα με την περίπτωση (σπανιότητα φαινομένου με συνεκτίμηση π.χ. της πυκνότητας του πληθυσμού, φύση και όγκος των δεδομένων, κ.λπ.). Αν ο έλεγχος αυτός δεν ικανοποιείται, τότε τα δεδομένα δεν έχουν ανωνυμοποιηθεί και, συνεπώς, παραμένουν στο πεδίο εφαρμογής του ΓΚΠΔ.

16 Η αξιολόγηση της αρτιότητας της ανωνυμοποίησης βασίζεται σε τρία κριτήρια: i) την απομόνωση της ταυτότητας ενός φυσικού προσώπου (από μία μεγαλύτερη ομάδα με βάση τα δεδομένα ξεχωρίζεται ένα άτομο)· ii) τη διασυνδεσιμότητα (διασύνδεση δύο στοιχείων που αφορούν το ίδιο άτομο)· και iii) την επαγωγή (συνάγονται, με σημαντική πιθανότητα, άγνωστες πληροφορίες για ένα άτομο).

17 Η έννοια της ανωνυμοποίησης είναι επιρρεπής σε παρανόηση και συχνά συγχέεται με την ψευδωνυμοποίηση. Ενώ η ανωνυμοποίηση επιτρέπει τη χρήση των δεδομένων χωρίς κανένα περιορισμό, τα ψευδωνυμοποιημένα δεδομένα εξακολουθούν να εμπίπτουν στο πεδίο εφαρμογής του ΓΚΠΔ.

18 Υπάρχουν πολλές επιλογές για αποτελεσματική ανωνυμοποίηση[9], αλλά με επιφυλάξεις. Τα δεδομένα δεν μπορούν να ανωνυμοποιηθούν μεμονωμένα —αυτό σημαίνει ότι μόνον ένα ολόκληρο σύνολο δεδομένων μπορεί να ανωνυμοποιηθεί ή όχι. Μ’ αυτήν την έννοια, κάθε παρέμβαση σε μια μοναδική σχηματομορφή δεδομένων (μέσω κρυπτογράφησης ή οποιουδήποτε άλλου μαθηματικού μετασχηματισμού) μπορεί στην καλύτερη περίπτωση να θεωρηθεί ψευδωνυμοποίηση.

19 Οι διεργασίες ανωνυμοποίησης και οι επιθέσεις εκ νέου ταυτοποίησης είναι ενεργά πεδία έρευνας. Για έναν υπεύθυνο επεξεργασίας που υλοποιεί λύσεις ανωνυμοποίησης έχει ζωτική σημασία να παρακολουθεί τις πρόσφατες εξελίξεις σ’ αυτόν τον τομέα, ιδίως όσον αφορά τα δεδομένα θέσης (που προέρχονται από τηλεπικοινωνιακούς φορείς εκμετάλλευσης και/ή υπηρεσίες της κοινωνίας των πληροφοριών) τα οποία είναι γνωστό ότι είναι εξαιρετικά δύσκολο να ανωνυμοποιηθούν.

20 Πράγματι, πάρα πολλές έρευνες έδειξαν[10] ότι *δεδομένα θέσης που θεωρείτο ότι είχαν ανωνυμοποιηθεί* ίσως να μην είχαν ανωνυμοποιηθεί στην πραγματικότητα. Τα ίχνη των μετακινήσεων των ατόμων από τη φύση τους συσχετίζονται μεταξύ τους και είναι μοναδικά. Ως εκ τούτου, μπορούν, υπό ορισμένες προϋποθέσεις, να είναι ευάλωτα σε προσπάθειες εκ νέου ταυτοποίησης.

21 Μια μοναδική σχηματομορφή δεδομένων που παρακολουθεί τη θέση ενός ατόμου για μια σημαντική χρονική περίοδο δεν μπορεί να ανωνυμοποιηθεί πλήρως. Η αξιολόγηση αυτή μπορεί να ισχύει ακόμη κι αν η ακρίβεια των καταγεγραμμένων γεωγραφικών συντεταγμένων δεν είναι επαρκώς μειωμένη ή αν οι λεπτομέρειες του ίχνους έχουν αφαιρεθεί και ακόμη κι αν διατηρούνται μόνον οι τοποθεσίες στις οποίες παρέμεινε το υποκείμενο των δεδομένων για σημαντικά χρονικά διαστήματα. Αυτό ισχύει επίσης για τα δεδομένα θέσης που δεν είναι επαρκώς συγκεντρωτικά.

22 Για να επιτευχθεί η ανωνυμοποίηση, πρέπει να γίνεται προσεκτική επεξεργασία των δεδομένων θέσης ώστε να ικανοποιείται ο έλεγχος εύλογου χαρακτήρα. Με αυτήν την έννοια, η επεξεργασία αυτού του τύπου περιλαμβάνει τον χειρισμό ολόκληρων των συνόλων δεδομένων θέσης, καθώς και την επεξεργασία δεδομένων από ένα ευλόγως μεγάλο σύνολο ατόμων με τη χρήση άρτιων τεχνικών ανωνυμοποίησης, υπό την προϋπόθεση ότι αυτές εφαρμόζονται επαρκώς και αποτελεσματικά.

---

[9] (de Montjoye et al., 2018) «On the privacy-conscientious use of mobile phone data»
[10] (de Montjoye et al., 2013) «Unique in the Crowd: The privacy bounds of human mobility» και (Pyrgelis et al., 2017) «Knock Knock, Who’s There? Membership Inference on Aggregate Location Data»

23 Τέλος, δεδομένης της πολυπλοκότητας των διεργασιών ανωνυμοποίησης, ενθαρρύνεται ιδιαίτερα η εξασφάλιση διαφάνειας όσον αφορά τη μεθοδολογία ανωνυμοποίησης.

3 ΕΦΑΡΜΟΓΕΣ ΙΧΝΗΛΑΤΗΣΗΣ ΕΠΑΦΩΝ

3.1 Γενική νομική ανάλυση

24 Η συστηματική, σε ευρεία κλίμακα, παρακολούθηση της θέσης και/ή των επαφών μεταξύ των φυσικών προσώπων συνιστά σοβαρή παραβίαση της ιδιωτικής ζωής τους. Μπορεί να νομιμοποιηθεί μόνο με την εκούσια έγκριση από τους χρήστες για καθέναν από τους σχετικούς σκοπούς. Αυτό σημαίνει, ειδικότερα, ότι τα άτομα που δεν επιλέγουν ή δεν μπορούν να κάνουν χρήση αυτών των εφαρμογών, δεν θα πρέπει να υφίστανται καμία συνέπεια.

25 Για τη διασφάλιση της λογοδοσίας θα πρέπει να ορίζεται σαφώς ο υπεύθυνος επεξεργασίας κάθε εφαρμογής ιχνηλάτησης επαφών. Το ΕΣΠΔ θεωρεί ότι οι εθνικές υγειονομικές αρχές θα μπορούσαν να είναι οι υπεύθυνοι επεξεργασίας[11] για μια τέτοια εφαρμογή· μπορούν επίσης να προβλεφθούν και άλλοι υπεύθυνοι επεξεργασίας. Σε κάθε περίπτωση, εάν η έναρξη διάθεσης των εφαρμογών ιχνηλάτησης επαφών προϋποθέτει τη συμμετοχή διάφορων συντελεστών, οι ρόλοι και οι ευθύνες τους πρέπει να καθορίζονται σαφώς εξ αρχής και να εξηγούνται στους χρήστες.

26 Επιπλέον, όσον αφορά την αρχή του περιορισμού του σκοπού, οι σκοποί πρέπει να είναι αρκετά συγκεκριμένοι ώστε να αποκλείεται η περαιτέρω επεξεργασία για σκοπούς που δεν συνδέονται με τη διαχείριση της κρίσης υγείας λόγω της COVID-19 (π.χ. για εμπορικούς σκοπούς ή για σκοπούς επιβολής του νόμου). Αφού καθοριστεί με σαφήνεια ο στόχος, θα χρειαστεί να εξασφαλιστεί ότι η χρήση των δεδομένων προσωπικού χαρακτήρα είναι κατάλληλη, αναγκαία και αναλογική.

27 Στο πλαίσιο μιας εφαρμογής ιχνηλάτησης επαφών, θα πρέπει να λαμβάνεται σχολαστικά υπόψη η αρχή της ελαχιστοποίησης των δεδομένων και της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού:

- για τις εφαρμογές ιχνηλάτησης επαφών δεν απαιτείται παρακολούθηση της θέσης μεμονωμένων χρηστών. Αντ' αυτού θα πρέπει να χρησιμοποιούνται δεδομένα προσέγγισης·
- δεδομένου ότι οι εφαρμογές ιχνηλάτησης επαφών μπορούν να λειτουργήσουν χωρίς την άμεση ταυτοποίηση των ατόμων, θα πρέπει να θεσπιστούν κατάλληλα μέτρα για την πρόληψη της εκ νέου ταυτοποίησης·
- οι συλλεγόμενες πληροφορίες θα πρέπει να παραμένουν στον τερματικό εξοπλισμό του χρήστη και μόνο οι σχετικές πληροφορίες θα πρέπει να συλλέγονται όταν είναι απολύτως απαραίτητο.

28 Όσον αφορά τη νομιμότητα της επεξεργασίας, το ΕΣΠΔ επισημαίνει ότι οι εφαρμογές ιχνηλάτησης επαφών περιλαμβάνουν την αποθήκευση και/ή την πρόσβαση σε πληροφορίες που είναι ήδη αποθηκευμένες στον τερματικό εξοπλισμό, οι οποίες εμπίπτουν στο άρθρο 5 παράγραφος 3 της οδηγίας. Εάν οι εν λόγω εργασίες είναι απολύτως απαραίτητες για την παροχή της υπηρεσίας που έχει ζητήσει ρητά ο χρήστης, η επεξεργασία δεν απαιτεί τη συγκατάθεσή του. Για τις πράξεις που δεν είναι απολύτως αναγκαίες, ο πάροχος θα πρέπει να ζητήσει τη συγκατάθεση του χρήστη.

29 Επιπλέον, το ΕΣΠΔ επισημαίνει ότι το γεγονός και μόνο ότι η χρήση εφαρμογών ιχνηλάτησης επαφών πραγματοποιείται σε οικειοθελή βάση δεν σημαίνει ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα θα βασιστεί αναγκαστικά στη συγκατάθεση. Όταν οι δημόσιες αρχές παρέχουν υπηρεσία βάσει εντολής που τους έχει ανατεθεί από τον νόμο και σύμφωνα με τις απαιτήσεις που ορίζει ο νόμος, φαίνεται ότι η πλέον κατάλληλη νομική βάση για την επεξεργασία είναι η αναγκαιότητα για την εκτέλεση καθήκοντος προς το δημόσιο συμφέρον, δηλαδή το άρθρο 6 παράγραφος 1 στοιχείο ε) του ΓΚΠΔ.

---

[11] Βλ. επίσης Ευρωπαϊκή Επιτροπή «Έγγραφο καθοδήγησης για τις εφαρμογές που στηρίζουν την καταπολέμηση της πανδημίας COVID-19 σε σχέση με την προστασία των δεδομένων», Βρυξέλλες, 16.4.2020 C (2020) 2523 final.

30 Το άρθρο 6 παράγραφος 3 του ΓΚΠΔ διευκρινίζει ότι η βάση της επεξεργασίας που αναφέρεται στο άρθρο 6 παράγραφος 1 στοιχείο ε) καθορίζεται από το δίκαιο της Ένωσης ή του κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας. Ο σκοπός της επεξεργασίας καθορίζεται στην εν λόγω νομική βάση ή, όσον αφορά την επεξεργασία που αναφέρεται στην παράγραφο 1 στοιχείο ε), αυτή είναι αναγκαία για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.[12]

31 Η νομική βάση ή το νομοθετικό μέτρο που παρέχει τη νόμιμη βάση για τη χρήση των εφαρμογών ιχνηλάτησης επαφών θα πρέπει, ωστόσο, να περιλαμβάνει ουσιαστικές διασφαλίσεις, συμπεριλαμβανομένης της αναφοράς στον οικειοθελή χαρακτήρα της εφαρμογής. Θα πρέπει να περιλαμβάνεται σαφής προσδιορισμός του σκοπού και ρητοί περιορισμοί σχετικά με την περαιτέρω χρήση των δεδομένων προσωπικού χαρακτήρα, καθώς και σαφής ταυτοποίηση του υπευθύνου ή των υπευθύνων επεξεργασίας. Θα πρέπει επίσης να προσδιορίζονται οι κατηγορίες δεδομένων, καθώς και οι οντότητες στις οποίες (και οι σκοποί για τους οποίους) μπορούν να γνωστοποιούνται τα δεδομένα προσωπικού χαρακτήρα. Ανάλογα με το επίπεδο της παρέμβασης, θα πρέπει να ενσωματώνονται πρόσθετες διασφαλίσεις, λαμβάνοντας υπόψη τη φύση, το πεδίο και τους σκοπούς της επεξεργασίας. Τέλος, το ΕΣΠΔ συνιστά επίσης να συμπεριληφθούν, το συντομότερο δυνατόν, τα κριτήρια που καθορίζουν πότε θα αποσυναρμολογηθεί η εφαρμογή και ποια οντότητα θα είναι υπεύθυνη και υπόλογη για την αποσυναρμολόγηση.

32 Ωστόσο, εάν η επεξεργασία των δεδομένων βασίζεται σε άλλη νομική βάση, όπως η συγκατάθεση [άρθρο 6 παράγραφος 1 στοιχείο α)][13] για παράδειγμα, ο υπεύθυνος επεξεργασίας πρέπει να διασφαλίζει ότι πληρούνται οι αυστηρές απαιτήσεις για την εγκυρότητα της εν λόγω νομικής βάσης.

33 Επιπλέον, η χρήση μιας εφαρμογής για την καταπολέμηση της πανδημίας COVID-19 ενδέχεται να οδηγήσει στη συλλογή δεδομένων για την υγεία (για παράδειγμα, η κατάσταση ενός ατόμου ως προς την προσβολή από τον ιό). Η επεξεργασία των δεδομένων αυτών επιτρέπεται όταν η επεξεργασία αυτή είναι απαραίτητη για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, που πληρούν τους όρους του άρθρου 9 παράγραφος 2 στοιχείο θ) του ΓΚΠΔ[14] ή για σκοπούς υγειονομικής περίθαλψης όπως περιγράφεται στο άρθρο 9 παράγραφος 2 στοιχείο η) του ΓΚΠΔ[15]. Ανάλογα με τη νομική βάση, μπορεί επίσης να βασίζεται σε ρητή συγκατάθεση [άρθρο 9 παράγραφος 2 στοιχείο α) του ΓΚΠΔ].

34 Σύμφωνα με τον αρχικό σκοπό, το άρθρο 9 παράγραφος 2 στοιχείο ι) του ΓΚΠΔ επιτρέπει επίσης την επεξεργασία δεδομένων που αφορούν την υγεία, όταν αυτό είναι αναγκαίο για σκοπούς επιστημονικής έρευνας ή στατιστικούς σκοπούς.

35 Η τρέχουσα κρίση στον τομέα της υγείας δεν θα πρέπει να χρησιμοποιηθεί ως ευκαιρία για τη θέσπιση δυσανάλογων εντολών διατήρησης δεδομένων. Ο περιορισμός της αποθήκευσης θα πρέπει να λαμβάνει υπόψη τις πραγματικές ανάγκες και την ιατρική σημασία (αυτό μπορεί να περιλαμβάνει επιδημιολογικούς παράγοντες όπως η περίοδος επώασης κ.λπ.) και τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να διατηρούνται μόνο για τη διάρκεια της κρίσης COVID-19. Στη συνέχεια, κατά γενικό κανόνα, όλα τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να διαγράφονται ή να ανωνυμοποιούνται.

36 Σύμφωνα με το πνεύμα του ΕΣΠΔ, οι εν λόγω εφαρμογές δεν μπορούν να αντικαταστήσουν, αλλά μόνο να στηρίξουν, τη μη ψηφιακή ιχνηλάτηση επαφών από ειδικευμένο προσωπικό του

[12] Βλ. αιτιολογική σκέψη 41.
[13] Οι υπεύθυνοι επεξεργασίας (ιδίως οι δημόσιες αρχές) πρέπει να δίνουν ιδιαίτερη προσοχή στο γεγονός ότι η συγκατάθεση δεν θα πρέπει να θεωρείται ότι δίνεται ελεύθερα, εάν το φυσικό πρόσωπο δεν έχει πραγματική επιλογή να αρνηθεί ή να αποσύρει τη συγκατάθεσή του χωρίς να ζημιωθεί.
[14] Η επεξεργασία πρέπει να βασίζεται στο δίκαιο της Ένωσης ή κράτους μέλους, το οποίο προβλέπει κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων, και ιδίως του επαγγελματικού απορρήτου.
[15] Βλ. άρθρο 9 παράγραφος 2 στοιχείο η) του ΓΚΠΔ.

τομέα δημόσιας υγείας, το οποίο μπορεί να διακρίνει κατά πόσον οι στενές επαφές είναι πιθανό να συνεπάγονται μετάδοση του ιού ή όχι (π.χ. όταν η αλληλεπίδραση αφορά άτομο που προστατεύεται από κατάλληλο εξοπλισμό —ταμίες κ.λπ.— ή όχι). Το ΕΣΠΔ υπογραμμίζει ότι οι διαδικασίες και οι διεργασίες, συμπεριλαμβανομένων των αντίστοιχων αλγορίθμων, που χρησιμοποιούν οι εφαρμογές ιχνηλάτησης επαφών θα πρέπει να λειτουργούν υπό την αυστηρή επίβλεψη ειδικευμένου προσωπικού, ώστε να περιορίζεται η εμφάνιση ψευδοθετικών και ψευδοαρνητικών αποτελεσμάτων. Ειδικότερα, το καθήκον της παροχής συμβουλών σχετικά με τα επόμενα βήματα δεν θα πρέπει να βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία.

37 Για να διασφαλιστεί ο δίκαιος χαρακτήρας, η λογοδοσία και, γενικότερα, η συμμόρφωσή τους με τη νομοθεσία, οι αλγόριθμοι πρέπει να υπόκεινται σε έλεγχο και θα πρέπει να επανεξετάζονται τακτικά από ανεξάρτητους εμπειρογνώμονες. Ο κώδικας πηγής της εφαρμογής θα πρέπει να δημοσιοποιείται για όσο το δυνατόν ευρύτερο έλεγχο.

38 Ψευδοθετικά αποτελέσματα πάντα θα εμφανίζονται σε κάποιο βαθμό. Επειδή η διαπίστωση ότι υπάρχει κίνδυνος λοίμωξης μπορεί να έχει σημαντικές συνέπειες για τα άτομα, όπως το ότι θα πρέπει να παραμείνουν σε αυτοαπομόνωση έως ότου αποδειχθεί ότι είναι αρνητικά, χρειάζεται να υπάρχει η δυνατότητα διόρθωσης των δεδομένων και/ή των αποτελεσμάτων των επακόλουθων αναλύσεων. Αυτό, φυσικά, θα πρέπει να ισχύει μόνο για σενάρια και υλοποιήσεις όπου τα δεδομένα υποβάλλονται σε επεξεργασία και/ή αποθηκεύονται με τρόπο που να είναι τεχνικά εφικτή τέτοιου είδους διόρθωση και όπου είναι πιθανόν να συμβούν οι αρνητικές συνέπειες που αναφέρονται ανωτέρω.

39 Τέλος, το ΕΣΠΔ θεωρεί ότι μια εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων (ΕΑΠΔ) πρέπει να διενεργείται πριν από την υλοποίηση ενός τέτοιου εργαλείου, δεδομένου ότι η επεξεργασία θεωρείται ότι ενέχει πιθανότατα υψηλό κίνδυνο (δεδομένα για την υγεία, αναμενόμενη χρήση σε ευρεία κλίμακα, συστηματική παρακολούθηση, χρήση νέων τεχνολογικών λύσεων)[16]. Το ΕΣΠΔ συνιστά ένθερμα τη δημοσίευση των ΕΑΠΔ.

3.2 Συστάσεις και λειτουργικές απαιτήσεις

40 Σύμφωνα με την αρχή της ελαχιστοποίησης των δεδομένων, μεταξύ άλλων μέτρων για την προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού[17], τα δεδομένα που υποβάλλονται σε επεξεργασία θα πρέπει να περιορίζονται στο απολύτως ελάχιστο. Η εφαρμογή δεν θα πρέπει να συλλέγει άσχετες ή αχρείαστες πληροφορίες, οι οποίες μπορεί να περιλαμβάνουν την οικογενειακή κατάσταση, αναγνωριστικά επικοινωνίας, στοιχεία των καταλόγων αρχείων στον εξοπλισμό, μηνύματα, μητρώα κλήσεων, δεδομένα θέσης, αναγνωριστικά συσκευής κ.λπ.

41 Τα δεδομένα που εκπέμπονται από τις εφαρμογές πρέπει να περιλαμβάνουν μόνο ορισμένα μοναδικά και ψευδωνυμοποιημένα αναγνωριστικά, που παράγονται από την εφαρμογή και αφορούν ειδικά την εν λόγω εφαρμογή. Αυτά τα αναγνωριστικά πρέπει να ανανεώνονται τακτικά, σε συχνότητα συμβατή με τον σκοπό του περιορισμού της διασποράς του ιού, και να επαρκούν ώστε να περιορίζουν τους κινδύνους ταυτοποίησης και φυσικού εντοπισμού των ατόμων.

42 Οι υλοποιήσεις για την ιχνηλάτηση επαφών μπορούν να ακολουθούν μια κεντρική ή μια αποκεντρωμένη προσέγγιση[18]. Και οι δύο προσεγγίσεις θα πρέπει να θεωρούνται βιώσιμες επιλογές, με την προϋπόθεση ότι εφαρμόζονται κατάλληλα μέτρα ασφάλειας, και καθεμία

[16] Βλ. WP29 Κατευθυντήριες γραμμές (εκδόθηκαν από το ΕΣΠΔ) για την εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και για να προσδιοριστεί κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679.
[17] Βλ. Κατευθυντήριες γραμμές αριθ. 4/2019 του ΕΣΠΔ σχετικά με το άρθρο 25 «Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού»
[18] Γενικά, η αποκεντρωμένη λύση συνάδει περισσότερο με την αρχή της ελαχιστοποίησης.

συνοδεύεται από ένα σύνολο πλεονεκτημάτων και μειονεκτημάτων. Συνεπώς, το στάδιο της μελέτης στην ανάπτυξη μιας εφαρμογής θα πρέπει να περιλαμβάνει πάντα τη διεξοδική εξέταση και των δύο πτυχών, δηλαδή την προσεκτική στάθμιση των σχετικών συνεπειών στην προστασία των δεδομένων/της ιδιωτικής ζωής και τις πιθανές επιπτώσεις για τα δικαιώματα των ατόμων.

43 Κάθε εξυπηρετητής που εμπλέκεται στο σύστημα ιχνηλάτησης επαφών πρέπει να συλλέγει μόνο το ιστορικό επαφών ή τα ψευδώνυμα αναγνωριστικά ενός χρήστη που έχει διαγνωστεί ως προσβεβλημένος, ως αποτέλεσμα κατάλληλης αξιολόγησης που πραγματοποιείται από τις υγειονομικές αρχές και οικειοθελούς ενέργειας του χρήστη. Εναλλακτικά, ο εξυπηρετητής πρέπει να τηρεί κατάλογο με τα ψευδώνυμα αναγνωριστικά των προσβεβλημένων χρηστών ή το ιστορικό επαφών τους μόνο για όσο χρόνο χρειάζεται για να ενημερώσει τους δυνητικά προσβεβλημένους χρήστες για την έκθεσή τους και δεν θα πρέπει να προσπαθεί να ταυτοποιήσει τους δυνητικά προσβεβλημένους χρήστες.

44 Η δημιουργία μιας μεθοδολογίας ολοκληρωμένης ιχνηλάτησης επαφών, που να περιλαμβάνει και εφαρμογές και μη ψηφιακή ιχνηλάτηση, ενδέχεται να απαιτεί την επεξεργασία πρόσθετων πληροφοριών σε ορισμένες περιπτώσεις. Σ’ αυτό το πλαίσιο, αυτές οι πρόσθετες πληροφορίες θα πρέπει να παραμένουν στον τερματικό εξοπλισμό του χρήστη και να υφίστανται επεξεργασία μόνον όταν είναι απολύτως αναγκαίο και μόνο με την προηγούμενη και ειδική συγκατάθεσή του.

45 Πρέπει να εφαρμόζονται εξελιγμένες κρυπτογραφικές τεχνικές για την προστασία των δεδομένων που είναι αποθηκευμένα σε εξυπηρετητές και σε εφαρμογές, και για την προστασία των ανταλλαγών δεδομένων μεταξύ εφαρμογών και απομακρυσμένων εξυπηρετητών. Πρέπει επίσης να εκτελείται αμοιβαία επαλήθευση ταυτότητας μεταξύ της εφαρμογής και του εξυπηρετητή.

46 Η αναφορά χρηστών ως προσβεβλημένων από τον SARS-CoV-2 πρέπει να υπόκειται σε κατάλληλη εξουσιοδότηση, για παράδειγμα μέσω ενός κωδικού μίας χρήσης που συνδέεται με ψευδώνυμη ταυτότητα του προσβεβλημένου προσώπου και συνδέεται με ένα υγειονομικό κέντρο ή επαγγελματία του τομέα της υγείας. Αν δεν είναι εφικτή η επιβεβαίωση με τρόπο ασφαλή, δεν θα πρέπει να γίνεται επεξεργασία δεδομένων που υποθέτει τη βεβαιότητα της κατάστασης του χρήστη.

47 Ο υπεύθυνος επεξεργασίας πρέπει, σε συνεργασία με τις δημόσιες αρχές, να ενημερώνει σαφώς και ρητά για τον σύνδεσμο από τον οποίο τηλεφορτώνεται η επίσημη εθνική εφαρμογή ιχνηλάτησης επαφών, ώστε να περιοριστεί ο κίνδυνος χρήσης εφαρμογών σχεδιασμένων από τρίτους.

4 ΣΥΜΠΕΡΑΣΜΑ

48 Ο κόσμος αντιμετωπίζει μια σημαντική κρίση στον τομέα της δημόσιας υγείας που απαιτεί ισχυρές απαντήσεις, οι οποίες θα έχουν αντίκτυπο και πέρα από την παρούσα κατάσταση έκτακτης ανάγκης. Η αυτοματοποιημένη επεξεργασία δεδομένων και οι ψηφιακές τεχνολογίες μπορούν να αποτελέσουν συνιστώσες στην καταπολέμηση της νόσου COVID-19. Ωστόσο, θα πρέπει να έχουμε υπόψη μας το «φαινόμενο της μη αναστρεψιμότητας». Είναι ευθύνη μας να εξασφαλίσουμε ότι κάθε μέτρο που λαμβάνεται σ’ αυτές τις εξαιρετικές περιστάσεις είναι αναγκαίο, έχει περιορισμένη διάρκεια και το ελάχιστο δυνατό εύρος, και υπόκειται σε περιοδική και πραγματική επανεξέταση καθώς και σε επιστημονική αξιολόγηση.

49 Το ΕΣΠΔ υπογραμμίζει ότι δεν θα έπρεπε να είμαστε αναγκασμένοι να επιλέξουμε ανάμεσα στην αποτελεσματική απάντηση στην τρέχουσα κρίση και στην προστασία των θεμελιωδών δικαιωμάτων μας: μπορούμε να επιτύχουμε και τα δύο, και επιπλέον οι βασικές αρχές που διέπουν την προστασία δεδομένων μπορούν να διαδραματίσουν πολύ σημαντικό ρόλο στην καταπολέμηση του ιού. Η ευρωπαϊκή νομοθεσία για την προστασία των δεδομένων επιτρέπει την υπεύθυνη χρήση δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της διαχείρισης της υγείας, ενώ διασφαλίζει επίσης ότι τα ατομικά δικαιώματα και οι ελευθερίες δεν συρρικνώνονται κατά τη διαδικασία.

Για το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Η Πρόεδρος

(Andrea Jelinek)

ΠΑΡΑΡΤΗΜΑ – ΕΦΑΡΜΟΓΕΣ ΙΧΝΗΛΑΤΗΣΗΣ ΕΠΑΦΩΝ ΟΔΗΓΟΣ ΑΝΑΛΥΣΗΣ

0. Δήλωση αποποίησης ευθύνης

Οι ακόλουθες κατευθυντήριες γραμμές δεν είναι ούτε περιοριστικές ούτε εξαντλητικές, και ο μοναδικός σκοπός του παρόντος οδηγού είναι να παράσχει γενική καθοδήγηση στους σχεδιαστές και τους φορείς υλοποίησης εφαρμογών ιχνηλάτησης επαφών. Και άλλες λύσεις, πέραν αυτών που περιγράφονται εδώ, μπορούν να χρησιμοποιηθούν και να είναι νόμιμες εφόσον συμμορφώνονται με το σχετικό νομικό πλαίσιο (δηλαδή τον ΓΚΠΔ και την οδηγία).

Πρέπει επίσης να σημειωθεί ότι ο παρών οδηγός είναι γενικού χαρακτήρα. Κατά συνέπεια, οι συστάσεις και οι υποχρεώσεις που παρατίθενται στο παρόν έγγραφο δεν πρέπει να θεωρούνται εξαντλητικές. Κάθε αξιολόγηση πρέπει να διενεργείται κατά περίπτωση και κάποιες εφαρμογές μπορεί να απαιτούν τη λήψη πρόσθετων μέτρων που δεν περιλαμβάνονται στον παρόντα οδηγό.

1. Συνοπτική παρουσίαση

Σε πολλά κράτη μέλη, οι εμπλεκόμενοι φορείς εξετάζουν το ενδεχόμενο να χρησιμοποιήσουν εφαρμογές *ιχνηλάτησης επαφών* που θα βοηθούν τους κατοίκους να διαπιστώνουν αν έχουν έρθει σε επαφή με άτομο προσβεβλημένο από τον ιό SARS-CoV-2.

Οι προϋποθέσεις υπό τις οποίες τέτοιες εφαρμογές θα μπορούσαν να συμβάλουν αποτελεσματικά στην αντιμετώπιση της πανδημίας δεν έχουν προσδιοριστεί ακόμη, και θα πρέπει να προσδιοριστούν πριν από οποιαδήποτε υλοποίηση μιας τέτοιας εφαρμογής. Ωστόσο, είναι σημαντικό να δοθούν κατευθυντήριες γραμμές που θα προσφέρουν σχετικές πληροφορίες στις ομάδες ανάπτυξης εφαρμογών, έτσι ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα ήδη από τα αρχικά στάδια του σχεδιασμού.

Πρέπει να σημειωθεί ότι ο παρών οδηγός είναι γενικού χαρακτήρα. Κατά συνέπεια, οι συστάσεις και οι υποχρεώσεις που παρατίθενται στο παρόν έγγραφο δεν πρέπει να θεωρούνται εξαντλητικές. Κάθε αξιολόγηση πρέπει να διενεργείται κατά περίπτωση και κάποιες εφαρμογές μπορεί να απαιτούν τη λήψη πρόσθετων μέτρων που δεν περιλαμβάνονται στον παρόντα οδηγό. Σκοπός του παρόντος οδηγού είναι να παράσχει γενική καθοδήγηση στους σχεδιαστές και τους φορείς υλοποίησης εφαρμογών ιχνηλάτησης επαφών.

Ορισμένα κριτήρια ενδέχεται να υπερβαίνουν τις αυστηρές απαιτήσεις που απορρέουν από το πλαίσιο προστασίας δεδομένων. Στόχος τους είναι να εξασφαλίσουν το υψηλότερο δυνατό επίπεδο διαφάνειας, προκειμένου να ενισχυθεί η κοινωνική αποδοχή αυτών των εφαρμογών ιχνηλάτησης επαφών.

Για τον σκοπό αυτό, οι εκδότες των εφαρμογών ιχνηλάτησης επαφών θα πρέπει να λαμβάνουν υπόψη τα ακόλουθα κριτήρια:

- Η χρήση μιας τέτοιας εφαρμογής πρέπει να είναι απολύτως οικειοθελής. Δεν επιτρέπεται να υποβάλλει σε περιορισμούς την πρόσβαση στα δικαιώματα που διασφαλίζονται από τον νόμο. Τα άτομα πρέπει να έχουν πλήρη έλεγχο επί των δεδομένων τους ανά πάσα στιγμή και θα πρέπει να μπορούν να επιλέγουν ελεύθερα αν θα κάνουν χρήση μιας τέτοιας εφαρμογής.

- Οι εφαρμογές ιχνηλάτησης επαφών πιθανότατα θα ενέχουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων και θα απαιτούν τη διενέργεια μιας εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων, προτού αρχίσουν να διατίθενται για χρήση.

- Είναι δυνατή η λήψη πληροφοριών σχετικά με προσεγγίσεις χρηστών της εφαρμογής χωρίς να εντοπίζεται η θέση των χρηστών. Αυτό το είδος εφαρμογής δεν απαιτεί τη χρήση δεδομένων θέσης και, ως εκ τούτου, δεν θα πρέπει να περιλαμβάνει τη χρήση τέτοιων δεδομένων.

- Όταν ένας χρήστης διαγιγνώσκεται ως προσβεβλημένος από τον ιό SARS-CoV-2, θα πρέπει να ειδοποιούνται μόνον τα άτομα με τα οποία ο χρήστης έχει έρθει σε στενή επαφή εντός της περιόδου φύλαξης των δεδομένων που είναι χρήσιμη, από επιδημιολογική άποψη, για την ιχνηλάτηση επαφών.

- Η λειτουργία των εφαρμογών αυτού του τύπου ενδέχεται να απαιτεί τη χρήση κεντρικού εξυπηρετητή, ανάλογα με την επιλεγείσα αρχιτεκτονική. Στην περίπτωση αυτή, και σύμφωνα με τις αρχές της ελαχιστοποίησης των δεδομένων και της προστασίας των δεδομένων εκ του σχεδιασμού, τα δεδομένα που υποβάλλονται σε επεξεργασία στον κεντρικό εξυπηρετητή θα πρέπει να περιορίζονται στα απολύτως ελάχιστα:

  - Όταν ένας χρήστης διαγιγνώσκεται ως προσβεβλημένος, μπορούν να συλλέγονται πληροφορίες σχετικά με τις προηγούμενες στενές επαφές του ή τα αναγνωριστικά που έχουν αποσταλεί από την εφαρμογή του χρήστη, μόνο με τη σύμφωνη γνώμη του χρήστη. Πρέπει να καθιερωθεί μια μέθοδος επαλήθευσης μέσω της οποίας να επιβεβαιώνεται ότι το άτομο έχει πράγματι προσβληθεί, χωρίς να ταυτοποιείται ο χρήστης. Από τεχνική άποψη, αυτό θα μπορούσε να επιτευχθεί με το να ειδοποιούνται οι επαφές μόνο μετά από παρέμβαση ενός επαγγελματία της υγείας, για παράδειγμα με τη χρήση ειδικού κωδικού μίας χρήσης.

  - Οι πληροφορίες που αποθηκεύονται στον κεντρικό εξυπηρετητή δεν θα πρέπει ούτε να επιτρέπουν στον υπεύθυνο επεξεργασίας να ταυτοποιεί τους χρήστες που έχουν διαγνωστεί ως προσβεβλημένοι ή έχουν έρθει σε επαφή με προσβεβλημένους χρήστες, ούτε να επιτρέπουν την αναγνώριση συνήθων τύπων επαφής που δεν χρειάζονται για την ανεύρεση των σχετικών επαφών.

- Η λειτουργία των εφαρμογών αυτού του τύπου απαιτεί την εκπομπή δεδομένων που διαβάζονται από συσκευές άλλων χρηστών, καθώς και τη λήψη τέτοιου είδους εκπεμπόμενων δεδομένων:

  - Αρκεί η ανταλλαγή ψευδώνυμων αναγνωριστικών μεταξύ των κινητών συσκευών των χρηστών (υπολογιστές, ταμπλέτες, συνδεδεμένα ρολόγια κ.λπ.), για παράδειγμα μέσω εκπομπής (π.χ. με τεχνολογία Bluetooth χαμηλής κατανάλωσης ενέργειας).

  - Τα αναγνωριστικά πρέπει να παράγονται με τη χρήση εξελιγμένων κρυπτογραφικών διεργασιών.

  - Τα αναγνωριστικά πρέπει να ανανεώνονται τακτικά ώστε να περιορίζεται ο κίνδυνος παρακολούθησης του φυσικού προσώπου ή επιθέσεων αποανωνυμοποίησης μέσω διασύνδεσης στοιχείων (linkage attacks).

- Οι εφαρμογές αυτού του είδους πρέπει να είναι ασφαλείς ώστε να προστατεύεται η ασφάλεια των τεχνικών διεργασιών. Συγκεκριμένα:
    - Η εφαρμογή δεν θα πρέπει να παρέχει στους χρήστες πληροφορίες που τους επιτρέπουν να συναγάγουν την ταυτότητα ή τη διάγνωση άλλων. Ο κεντρικός εξυπηρετητής δεν θα πρέπει ούτε να ταυτοποιεί τους χρήστες ούτε να συνάγει πληροφορίες σχετικά με αυτούς.

Δήλωση αποποίησης ευθύνης: Οι ανωτέρω αρχές αφορούν αποκλειστικά και μόνο τον δηλούμενο σκοπό των εφαρμογών *ιχνηλάτησης επαφών*, οι οποίες αποσκοπούν στην αυτόματη πληροφόρηση των ατόμων που ενδέχεται να έχουν εκτεθεί στον ιό (χωρίς να χρειάζεται ταυτοποίησή τους). Η λειτουργία και οι υποδομές της εφαρμογής μπορούν να ελέγχονται από την αρμόδια εποπτική αρχή. Η τήρηση του συνόλου ή μέρους αυτών των κατευθυντήριων γραμμών δεν είναι απαραίτητο ότι επαρκεί για την πλήρη συμμόρφωση με το νομοθετικό πλαίσιο προστασίας δεδομένων.

2. Ορισμοί

Επαφή	Για τις εφαρμογές ιχνηλάτησης επαφών, ως επαφή καλείται ένας χρήστης που έχει αλληλεπιδράσει με χρήστη ο οποίος είναι επιβεβαιωμένα φορέας του ιού, με διάρκεια και σε απόσταση τέτοια που να συνεπάγεται κίνδυνο σημαντικής έκθεσης σε λοίμωξη από τον ιό. Οι παράμετροι για τη διάρκεια της έκθεσης και την απόσταση μεταξύ των ατόμων πρέπει να προσδιορίζονται από τις υγειονομικές αρχές και μπορούν να ρυθμίζονται στην εφαρμογή.
Δεδομένα θέσης	Είναι όλα τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών ή από υπηρεσία ηλεκτρονικών επικοινωνιών, και τα οποία περιγράφουν τη γεωγραφική θέση του τερματικού εξοπλισμού ενός χρήστη μιας υπηρεσίας ηλεκτρονικών επικοινωνιών διαθέσιμης στο κοινό (όπως ορίζεται στην οδηγία), καθώς και δεδομένα από άλλες πιθανές πηγές, τα οποία αφορούν: - το γεωγραφικό πλάτος, το γεωγραφικό μήκος ή το υψόμετρο του τερματικού εξοπλισμού, - την κατεύθυνση κίνησης του χρήστη, ή - τον χρόνο καταγραφής των πληροφοριών θέσης.
Αλληλεπίδραση	Για τις εφαρμογές ιχνηλάτησης επαφών, ως αλληλεπίδραση ορίζεται η ανταλλαγή πληροφοριών μεταξύ δύο συσκευών που βρίσκονται πολύ κοντά μεταξύ τους (στον χώρο και τον χρόνο), εντός της εμβέλειας της χρησιμοποιούμενης τεχνολογίας επικοινωνίας (π.χ. Bluetooth). Ο ορισμός αυτός δεν περιλαμβάνει τη θέση των δύο χρηστών της αλληλεπίδρασης.
Φορέας ιού	Στο παρόν έγγραφο, φορείς του ιού θεωρούνται οι χρήστες που έχουν δώσει θετικό αποτέλεσμα σε εξέταση για τον ιό και έχουν λάβει επίσημη διάγνωση από ιατρό ή κέντρο υγείας.

Ιχνηλάτηση επαφών	Τα άτομα που έχουν έρθει σε στενή επαφή (σύμφωνα με κριτήρια που θα καθοριστούν από τους επιδημιολόγους) με άτομο προσβεβλημένο από τον ιό διατρέχουν σημαντικό κίνδυνο να προσβληθούν και τα ίδια και να μεταδώσουν τον ιό σε άλλους. Η ιχνηλάτηση επαφών είναι μια μεθοδολογία ελέγχου νόσων, κατά την οποία δημιουργείται κατάλογος όλων των ατόμων που έχουν προσεγγίσει φορέα του ιού, προκειμένου να διαπιστωθεί κατά πόσον αυτά διατρέχουν κίνδυνο λοίμωξης και να ληφθούν τα κατάλληλα υγειονομικά μέτρα γι’ αυτά.

3. Γενικά

GEN-1	Η εφαρμογή πρέπει να είναι εργαλείο συμπληρωματικό στις συμβατικές τεχνικές ιχνηλάτησης επαφών (κυρίως τις συνεντεύξεις με προσβεβλημένα άτομα), δηλαδή να αποτελεί μέρος ενός ευρύτερου προγράμματος για τη δημόσια υγεία. Θα πρέπει να χρησιμοποιηθεί μόνο έως ότου καταστεί εφικτή η διαχείριση των νέων λοιμώξεων με μη ψηφιακές τεχνικές ιχνηλάτησης επαφών μόνο.
GEN-2	Το αργότερο μέχρι να αποφασιστεί από τις αρμόδιες δημόσιες αρχές η «επάνοδος στην κανονική κατάσταση», θα πρέπει να έχει τεθεί σε εφαρμογή μια διαδικασία με την οποία θα τερματίζεται η συλλογή αναγνωριστικών (καθολική απενεργοποίηση της εφαρμογής, οδηγίες για την απεγκατάσταση της εφαρμογής, αυτόματη απεγκατάσταση κ.λπ.) και θα ενεργοποιείται η διαγραφή όλων των δεδομένων που έχουν συλλεχθεί, από όλες τις βάσεις δεδομένων (εφαρμογές κινητών συσκευών και εξυπηρετητές).
GEN-3	Ο κώδικας πηγής της εφαρμογής και του λογισμικού παρασκηνίου (backend) πρέπει να είναι ανοικτός, και οι τεχνικές προδιαγραφές τους πρέπει να δημοσιοποιούνται, έτσι ώστε κάθε ενδιαφερόμενος να μπορεί να ελέγχει τον κώδικα και να συνεισφέρει, όπου χρειάζεται, στη βελτίωση του κώδικα, στη διόρθωση τυχόν σφαλμάτων και στη διασφάλιση της διαφάνειας κατά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα.
GEN-4	Τα στάδια της έναρξης διάθεσης της εφαρμογής πρέπει να καθιστούν δυνατή τη σταδιακή επικύρωση της αποτελεσματικότητάς της από άποψη δημόσιας υγείας. Για τον σκοπό αυτόν θα πρέπει να καθορίζεται από την αρχή ένα πρωτόκολλο αξιολόγησης, το οποίο θα προσδιορίζει δείκτες που επιτρέπουν τη μέτρηση της αποτελεσματικότητας της εφαρμογής.

4. Σκοποί

PUR-1	Η εφαρμογή πρέπει να έχει ως μοναδικό σκοπό την ιχνηλάτηση επαφών, ώστε τα άτομα που ενδέχεται να έχουν εκτεθεί στον ιό SARS-CoV-2 να μπορούν να ειδοποιηθούν και να λάβουν περίθαλψη. Δεν πρέπει να χρησιμοποιείται για άλλους σκοπούς.

PUR-2	Η εφαρμογή δεν πρέπει να εκτρέπεται από την κύρια χρήση της και να χρησιμοποιείται με σκοπό την παρακολούθηση της συμμόρφωσης με μέτρα καραντίνας ή εγκλεισμού και/ή με την κοινωνική αποστασιοποίηση.
PUR-3	Η εφαρμογή δεν πρέπει να χρησιμοποιείται για την εξαγωγή συμπερασμάτων σχετικά με τη θέση των χρηστών με βάση τις αλληλεπιδράσεις τους και/ή με άλλα μέσα.

5. Ζητήματα λειτουργίας

FUNC-1	Η εφαρμογή πρέπει να παρέχει μια λειτουργία που να επιτρέπει την ειδοποίηση των χρηστών που ενδέχεται να έχουν εκτεθεί στον ιό, με βάση την προσέγγισή τους σε προσβεβλημένο χρήστη εντός διαστήματος Χ ημερών πριν από τη θετική εξέταση διαλογής (η τιμή Χ καθορίζεται από τις υγειονομικές αρχές).
FUNC-2	Η εφαρμογή θα πρέπει να παρέχει συστάσεις στους χρήστες που ενδέχεται να έχουν εκτεθεί στον ιό. Θα πρέπει να παρέχει οδηγίες σχετικά με τις περαιτέρω ενέργειες και σχετικά με τρόπους αναζήτησης συμβουλών. Σε τέτοιες περιπτώσεις, η παρέμβαση ανθρώπου θα είναι υποχρεωτική.
FUNC-3	Ο αλγόριθμος που θα υπολογίζει τον κίνδυνο λοίμωξης, εξετάζοντας τους παράγοντες της απόστασης και του χρόνου και, βάσει αυτών, αποφασίζοντας κατά πόσον κάποια επαφή θα πρέπει να καταγραφεί στον κατάλογο ιχνηλάτησης επαφών, πρέπει να παρέχει δυνατότητα ρύθμισης με ασφάλεια, ώστε να λαμβάνει υπόψη τις πλέον πρόσφατες γνώσεις σχετικά με την εξάπλωση του ιού.
FUNC-4	**Οι χρήστες πρέπει να ειδοποιούνται σε περίπτωση που έχουν εκτεθεί στον ιό** ή να ενημερώνονται τακτικά σχετικά με το αν έχουν εκτεθεί στον ιό ή όχι, εντός της περιόδου επώασης του ιού.
FUNC-5	Η εφαρμογή θα πρέπει να είναι διαλειτουργική με άλλες εφαρμογές που αναπτύσσονται σε όλα τα κράτη μέλη, ώστε οι χρήστες που ταξιδεύουν σε άλλα κράτη μέλη να μπορούν να ειδοποιούνται αποτελεσματικά.

6. Δεδομένα

DATA-1	Η εφαρμογή πρέπει να μπορεί να μεταδίδει και να λαμβάνει δεδομένα μέσω τεχνολογιών επικοινωνίας γειτνίασης, όπως η τεχνολογία Bluetooth χαμηλής κατανάλωσης ενέργειας, ώστε να είναι δυνατή η ιχνηλάτηση επαφών.
DATA-2	Τα εν λόγω εκπεμπόμενα δεδομένα πρέπει να περιλαμβάνουν ψευδοτυχαία αναγνωριστικά με ισχυρή κρυπτογράφηση, που να παράγονται από την εφαρμογή και να είναι ειδικά για αυτήν.
DATA-3	Ο κίνδυνος διένεξης μεταξύ ψευδοτυχαίων αναγνωριστικών θα πρέπει να είναι αρκετά χαμηλός.

DATA-4	Τα ψευδοτυχαία αναγνωριστικά πρέπει να ανανεώνονται τακτικά, με συχνότητα επαρκή ώστε να περιορίζεται ο κίνδυνος εκ νέου ταυτοποίησης, φυσικής παρακολούθησης ή αποανωνυμοποίησης των ατόμων μέσω διασύνδεσης στοιχείων, από οποιονδήποτε, συμπεριλαμβανομένων των χειριστών των κεντρικών εξυπηρετητών, άλλων χρηστών της εφαρμογής ή κακόβουλων τρίτων. Τα αναγνωριστικά πρέπει να παράγονται από την εφαρμογή του χρήστη, ενδεχομένως βάσει φύτρων (seeds) που παρέχονται από τον κεντρικό εξυπηρετητή.
DATA-5	Σύμφωνα με την αρχή της ελαχιστοποίησης των δεδομένων, η εφαρμογή δεν πρέπει να συλλέγει δεδομένα πέραν εκείνων που είναι απολύτως απαραίτητα για την ιχνηλάτηση επαφών.
DATA-6	Η εφαρμογή δεν πρέπει να συλλέγει δεδομένα θέσης με σκοπό την ιχνηλάτηση επαφών. Η χρήση δεδομένων θέσης επιτρέπεται αποκλειστικά για τον σκοπό της αλληλεπίδρασης με παρόμοιες εφαρμογές σε άλλες χώρες και η ακρίβειά της θα πρέπει να περιορίζεται στην απολύτως αναγκαία για τον συγκεκριμένο σκοπό.
DATA-7	Η εφαρμογή δεν θα πρέπει να συλλέγει δεδομένα υγείας πέραν εκείνων που είναι απολύτως απαραίτητα για τους σκοπούς της εφαρμογής, παρά μόνο σε προαιρετική βάση και με αποκλειστικό σκοπό την υποβοήθηση της διαδικασίας λήψης απόφασης για την ειδοποίηση του χρήστη.
DATA-8	Οι χρήστες πρέπει να ενημερώνονται για όλα τα δεδομένα προσωπικού χαρακτήρα που θα συλλέγονται. Τα δεδομένα αυτά θα πρέπει να συλλέγονται μόνο με την άδεια του χρήστη.

7. Τεχνικές ιδιότητες

TECH-1	Η εφαρμογή θα πρέπει να χρησιμοποιεί διαθέσιμες τεχνολογίες, όπως τεχνολογίες επικοινωνίας γειτνίασης (π.χ. Bluetooth χαμηλής κατανάλωσης ενέργειας), προκειμένου να εντοπίζει χρήστες που βρίσκονται κοντά στη συσκευή όπου εκτελείται η εφαρμογή.
TECH-2	Η εφαρμογή θα πρέπει να φυλάσσει στον εξοπλισμό το ιστορικό των επαφών του χρήστη, για προκαθορισμένο και περιορισμένο χρονικό διάστημα.
TECH-3	Η εφαρμογή μπορεί να βασίζεται σε κεντρικό εξυπηρετητή για την εκτέλεση ορισμένων λειτουργιών της.
TECH-4	Η εφαρμογή πρέπει να βασίζεται σε μια αρχιτεκτονική που θα εξαρτάται όσο το δυνατόν περισσότερο από τις συσκευές των χρηστών.
TECH-5	Με πρωτοβουλία των χρηστών που δηλώνονται ως προσβεβλημένοι από τον ιό και κατόπιν επιβεβαίωσης της κατάστασής τους από δεόντως πιστοποιημένο επαγγελματία της υγείας, το ιστορικό επαφών τους ή τα δικά τους αναγνωριστικά θα πρέπει να διαβιβάζονται στον κεντρικό εξυπηρετητή.

8. Ασφάλεια

SEC-1	Ένας μηχανισμός πρέπει να επαληθεύει την κατάσταση των χρηστών που δηλώνονται ως θετικοί για SARS-CoV-2 στην εφαρμογή, π.χ. παρέχοντας έναν κωδικό μίας χρήσης που συνδέεται με έναν ορισμένο σταθμό εξέτασης ή επαγγελματία της υγείας. Εάν δεν είναι δυνατή η λήψη επιβεβαίωσης με ασφαλή τρόπο, τα δεδομένα δεν πρέπει να υποβάλλονται σε επεξεργασία.
SEC-2	Τα δεδομένα που αποστέλλονται στον κεντρικό εξυπηρετητή πρέπει να διαβιβάζονται μέσω ασφαλούς διαύλου. Η χρήση υπηρεσιών ειδοποίησης που προσφέρονται από παρόχους πλατφορμών λειτουργικών συστημάτων θα πρέπει να αξιολογείται προσεκτικά και δεν θα πρέπει να οδηγεί σε αποκάλυψη οποιωνδήποτε δεδομένων σε τρίτους.
SEC-3	Τα αιτήματα δεν πρέπει να είναι ευάλωτα σε παραποίηση από κακόβουλους χρήστες.
SEC-4	Πρέπει να εφαρμόζονται εξελιγμένες τεχνικές κρυπτογράφησης για την προστασία της ανταλλαγής πληροφοριών μεταξύ της εφαρμογής και του εξυπηρετητή και μεταξύ των εφαρμογών και, κατά γενικό κανόνα, για την προστασία των πληροφοριών που βρίσκονται αποθηκευμένες στις εφαρμογές και στον εξυπηρετητή. Παραδείγματα τεχνικών που μπορούν να χρησιμοποιηθούν είναι: συμμετρική και ασύμμετρη κρυπτογράφηση, συναρτήσεις κατακερματισμού, έλεγχος ιδιωτικής συμμετοχής (private membership test), τομή ιδιωτικών συνόλων (private set intersection), φίλτρα Bloom, ιδιωτική ανάκτηση πληροφοριών, ομομορφική κρυπτογράφηση κ.λπ.
SEC-5	Ο κεντρικός εξυπηρετητής δεν πρέπει να τηρεί τα αναγνωριστικά σύνδεσης δικτύου (π.χ. διευθύνσεις IP) των χρηστών, συμπεριλαμβανομένων εκείνων που έχουν διαγνωστεί θετικά και οι οποίοι έχουν διαβιβάσει το ιστορικό των επαφών τους ή τα δικά τους αναγνωριστικά.
SEC-6	Για να αποφευχθεί η πλαστοπροσωπία ή η δημιουργία ψεύτικων χρηστών, ο εξυπηρετητής πρέπει να πραγματοποιεί επαλήθευση ταυτότητας της εφαρμογής.
SEC-7	Η εφαρμογή πρέπει να πραγματοποιεί επαλήθευση ταυτότητας του κεντρικού εξυπηρετητή.
SEC-8	Οι λειτουργίες του εξυπηρετητή θα πρέπει να προστατεύονται από επιθέσεις επαναληπτικής εκτέλεσης (replay attacks).
SEC-9	Οι πληροφορίες που διαβιβάζονται από τον κεντρικό εξυπηρετητή πρέπει να υπογράφονται ώστε να επαληθεύεται η προέλευση και η ακεραιότητά τους.
SEC-10	Η πρόσβαση σε όλα τα δεδομένα που αποθηκεύονται στον κεντρικό εξυπηρετητή και δεν είναι δημόσια, πρέπει να περιορίζεται μόνο στα εξουσιοδοτημένα πρόσωπα.
SEC-11	Ο διαχειριστής αδειών της συσκευής, σε επίπεδο λειτουργικού συστήματος, πρέπει να ζητά μόνο τις άδειες που είναι απαραίτητες για την πρόσβαση και τη χρήση των υπομονάδων επικοινωνίας, όποτε χρειάζεται, για την αποθήκευση των δεδομένων στον τερματικό εξοπλισμό και για την ανταλλαγή πληροφοριών με τον κεντρικό εξυπηρετητή.

9. Προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής των φυσικών προσώπων

Υπενθύμιση: οι ακόλουθες κατευθυντήριες γραμμές αφορούν εφαρμογή της οποίας μοναδικός σκοπός είναι η ιχνηλάτηση επαφών.

PRIV-1	Οι ανταλλαγές δεδομένων πρέπει να σέβονται την ιδιωτική ζωή των χρηστών (και ιδίως να τηρούν την αρχή της ελαχιστοποίησης των δεδομένων).
PRIV-2	Η εφαρμογή δεν πρέπει να επιτρέπει την άμεση ταυτοποίηση των χρηστών κατά τη χρήση της.
PRIV-3	Η εφαρμογή δεν πρέπει να επιτρέπει την παρακολούθηση των κινήσεων των χρηστών.
PRIV-4	Η χρήση της εφαρμογής δεν θα πρέπει να επιτρέπει στους χρήστες να πληροφορούνται οτιδήποτε αφορά άλλους χρήστες (και ιδίως εάν εκείνοι είναι φορείς του ιού ή όχι).
PRIV-5	Η εμπιστοσύνη στον κεντρικό εξυπηρετητή πρέπει να είναι περιορισμένη. Η διαχείριση του κεντρικού εξυπηρετητή πρέπει να τηρεί σαφώς καθορισμένους κανόνες διακυβέρνησης και να περιλαμβάνει όλα τα αναγκαία μέτρα για την προστασία της ασφάλειάς του. Η θέση του κεντρικού εξυπηρετητή θα πρέπει να επιτρέπει την αποτελεσματική εποπτεία από την αρμόδια εποπτική αρχή.
PRIV-6	Πρέπει να διενεργηθεί και να δημοσιοποιηθεί εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων.
PRIV-7	Η εφαρμογή θα πρέπει να αποκαλύπτει στον χρήστη μόνο το εάν αυτός έχει εκτεθεί στον ιό και, ει δυνατόν χωρίς να αποκαλύπτει πληροφορίες για άλλους χρήστες, πόσες φορές και σε ποιες ημερομηνίες εκτέθηκε.
PRIV-8	Οι πληροφορίες που παρέχονται από την εφαρμογή δεν πρέπει να επιτρέπουν στους χρήστες να ταυτοποιούν χρήστες που φέρουν τον ιό, ούτε να γνωρίζουν τις μετακινήσεις τους.
PRIV-9	Οι πληροφορίες που παρέχονται από την εφαρμογή δεν πρέπει να επιτρέπουν στις υγειονομικές αρχές να ταυτοποιούν, χωρίς τη συγκατάθεσή τους, χρήστες που έχουν ενδεχομένως εκτεθεί.
PRIV-10	Τα αιτήματα που υποβάλλονται από την εφαρμογή στον κεντρικό εξυπηρετητή δεν πρέπει να αποκαλύπτουν τίποτα για τον φορέα του ιού.
PRIV-11	Τα αιτήματα που υποβάλλονται από την εφαρμογή στον κεντρικό εξυπηρετητή δεν πρέπει να αποκαλύπτουν καμία περιττή πληροφορία σχετικά με τον χρήστη, παρά μόνον, ενδεχομένως, τα ψευδώνυμα αναγνωριστικά του και τον κατάλογο επαφών του, και μόνον όταν αυτό είναι αναγκαίο.
PRIV-12	Δεν πρέπει να είναι δυνατές οι επιθέσεις διασύνδεσης στοιχείων.
PRIV-13	Οι χρήστες πρέπει να είναι σε θέση να ασκούν τα δικαιώματά τους μέσω της εφαρμογής.
PRIV-14	Η διαγραφή της εφαρμογής πρέπει να έχει ως αποτέλεσμα τη διαγραφή όλων των δεδομένων που έχουν συλλεχθεί σε τοπικό επίπεδο.

PRIV-15	Η εφαρμογή θα πρέπει να συλλέγει μόνο δεδομένα που εκπέμπονται από εκτελέσεις της εφαρμογής ή ισοδύναμων διαλειτουργικών εφαρμογών. Δεν συλλέγονται δεδομένα σχετικά με άλλες εφαρμογές και/ή συσκευές επικοινωνίας γειτνίασης.
PRIV-16	Προκειμένου να αποφεύγεται η εκ νέου ταυτοποίηση από τον κεντρικό εξυπηρετητή, θα πρέπει να υλοποιούνται εξυπηρετητές μεσολάβησης. Σκοπός αυτών των *μη συμπραττόντων (non-colluding) εξυπηρετητών* είναι η ομαδοποίηση των αναγνωριστικών πολλών διαφορετικών χρηστών (τόσο φορέων του ιού όσο και χρηστών που υποβάλλουν αιτήματα) προτού αυτά κοινοποιηθούν στον κεντρικό εξυπηρετητή, ώστε ο κεντρικός εξυπηρετητής να μην είναι σε θέση να γνωρίζει τα αναγνωριστικά (π.χ. διευθύνσεις IP) των χρηστών.
PRIV-17	Η εφαρμογή και ο εξυπηρετητής πρέπει να αναπτυχθούν και να διαμορφωθούν προσεκτικά έτσι ώστε να μη συλλέγουν περιττά δεδομένα (π.χ. δεν θα πρέπει να περιλαμβάνονται αναγνωριστικά στα αρχεία καταγραφής των εξυπηρετητών κ.λπ.) και ώστε να αποφεύγεται η χρήση κιτ ανάπτυξης λογισμικού (SDK) τρίτων που συλλέγουν δεδομένα για άλλους σκοπούς.

Οι περισσότερες εφαρμογές ιχνηλάτησης επαφών που συζητούνται επί του παρόντος ακολουθούν βασικά δύο προσεγγίσεις όσον αφορά τους χρήστες που χαρακτηρίζονται προσβεβλημένοι: μπορούν είτε να αποστέλλουν στον εξυπηρετητή το ιστορικό των επαφών προσέγγισης που έχουν λάβει μέσω σάρωσης, είτε να αποστέλλουν τον κατάλογο των αναγνωριστικών που εξέπεμψαν οι ίδιες. Περιγράφονται οι παρακάτω αρχές, ανάλογα με τις δύο αυτές προσεγγίσεις. Αυτές οι προσεγγίσεις εξετάζονται εδώ, αλλά αυτό δεν σημαίνει ότι άλλες προσεγγίσεις δεν είναι εφικτές ή ακόμη και προτιμότερες, όπως για παράδειγμα προσεγγίσεις που εφαρμόζουν κάποια μορφή κρυπτογράφησης E2E ή άλλες τεχνολογίες για την ενίσχυση της ασφάλειας ή της προστασίας της ιδιωτικής ζωής.

9.1. **Αρχές που εφαρμόζονται** μόνον **όταν η εφαρμογή αποστέλλει στον εξυπηρετητή έναν κατάλογο επαφών:**

CON-1	Ο κεντρικός εξυπηρετητής πρέπει να συλλέγει, κατόπιν οικειοθελούς ενέργειάς τους, το ιστορικό επαφών των χρηστών που δηλώνονται ως θετικοί στον SARS-CoV-2.
CON-2	Ο κεντρικός εξυπηρετητής δεν πρέπει να διατηρεί ούτε να διανέμει κατάλογο με τα ψευδώνυμα αναγνωριστικά των χρηστών που φέρουν τον ιό.
CON-3	Το ιστορικό επαφών που είναι αποθηκευμένο στον κεντρικό εξυπηρετητή πρέπει να διαγράφεται αφού οι χρήστες ειδοποιηθούν για την προσέγγισή τους σε άτομο που έχει λάβει θετική διάγνωση.
CON-4	Με εξαίρεση τις περιπτώσεις όπου ο χρήστης, που έχει βρεθεί θετικός, μοιράζεται το ιστορικό επαφών του με τον κεντρικό εξυπηρετητή, ή όπου ο χρήστης υποβάλλει αίτημα στον εξυπηρετητή για να πληροφορηθεί τυχόν έκθεσή του στον ιό, δεν επιτρέπεται να αποστέλλονται δεδομένα από τον εξοπλισμό του χρήστη.
CON-5	Κάθε αναγνωριστικό που περιλαμβάνεται στο τοπικό ιστορικό πρέπει να διαγράφεται μετά την παρέλευση X ημερών από τη συλλογή του (η τιμή X καθορίζεται από τις υγειονομικές αρχές).

CON-6	Το ιστορικό επαφών που αποστέλλεται από διαφορετικούς χρήστες δεν θα πρέπει να υποβάλλεται σε περαιτέρω επεξεργασία, π.χ. διασταύρωση με σκοπό την κατάρτιση γενικών χαρτών προσέγγισης.
CON-7	Τα δεδομένα που περιέχονται στα αρχεία καταγραφής των εξυπηρετητών πρέπει να περιορίζονται στο ελάχιστο δυνατό και πρέπει να συμμορφώνονται με τις απαιτήσεις προστασίας των δεδομένων.

9.2. Αρχές που εφαρμόζονται μόνον όταν η εφαρμογή αποστέλλει στον εξυπηρετητή έναν κατάλογο των δικών της αναγνωριστικών:

ID-1	Ο κεντρικός εξυπηρετητής πρέπει να συλλέγει, κατόπιν οικειοθελούς ενέργειάς τους, τα αναγνωριστικά που εκπέμπονται από τις εφαρμογές των χρηστών που δηλώνονται ως θετικοί στον SARS-CoV-2.
ID-2	Ο κεντρικός εξυπηρετητής δεν πρέπει να διατηρεί ούτε να διανέμει το ιστορικό επαφών των χρηστών που φέρουν τον ιό.
ID-3	Τα αναγνωριστικά που βρίσκονται αποθηκευμένα στον κεντρικό εξυπηρετητή πρέπει να διαγράφονται αφού διανεμηθούν στις άλλες εφαρμογές.
ID-4	Με εξαίρεση τις περιπτώσεις όπου ο χρήστης, που έχει βρεθεί θετικός, μοιράζεται τα αναγνωριστικά του με τον κεντρικό εξυπηρετητή, ή όπου ο χρήστης υποβάλλει αίτημα στον εξυπηρετητή για να πληροφορηθεί τυχόν έκθεσή του στον ιό, δεν επιτρέπεται να αποστέλλονται δεδομένα από τον εξοπλισμό του χρήστη.
ID-5	Τα δεδομένα που περιέχονται στα αρχεία καταγραφής των εξυπηρετητών πρέπει να περιορίζονται στο ελάχιστο δυνατό και πρέπει να συμμορφώνονται με τις απαιτήσεις προστασίας των δεδομένων.